IN THE CLAIMS

1-29. (cancelled)

30. (currently amended) A method for distributively and dynamically securing a communications network, comprising the steps of:

interconnecting a network device between each computer equipment to be secured and the network;

intercepting communications between a computer equipment connected to said device and the network by said device;

obtaining information related to a user of said computer equipment by an authentication module associated with said device;

defining a security level of said device by said authentication module associated with said device;

transmitting said information related to the user and said security level of said device to an authentication management server connected to the network,

authenticating the user by said authentication management server in accordance with said information related to the user and said security level of said device;

distributively transmitting security parameters from ~~the~~ said authentication management server to ~~each~~ devices on the network;

storing said security parameters by each device; and

processing, in each device, said security parameters received from said authentication management server, thereby distributively and dynamically configuring the security of the network to address new modes of attack.

31. (previously added) The method of claim 30, wherein said security parameters comprise a list of authorized computer client/server applications and information enabling each device to analyze messages related to said client/server applications.

32. (previously added) The method of claim 31, further comprising the steps of:

analyzing the messages related to said client/server applications by said device;

filtering the messages related to said client/server applications by said device; and

altering the messages related to said client/server applications by said device, thereby establishing a firewall.

33. (previously added) The method of claim 30, wherein said security parameters comprise a list of computer equipment which the user is authorized to communicate with.

34. (previously added) The method of claim 33, further comprising the steps of:

enabling said device to transmit messages between said computer equipment associated with the user and a computer equipment on said list; and

blocking said device from transmitting messages between said computer associated with the user and a computer equipment not on said list.

35. (previously added) The method of claim 30, further comprising the steps of:

customizing said device in accordance with a private encipherment key provided by said authentication module;

storing public encipherment keys associated with private encipherment keys which customize the devices by said server.

36. (previously added) The method of claim 35, wherein said security parameters comprise a list of computer equipment and the corresponding public encipherment key which the user is authorized to communicate with, in an enciphered manner.

37. (previously added) The method of claim 36, further comprising the step of enciphering by said device communications between said computer equipment associated with the user and a computer equipment on said list by combining the private encipherment key of said device with the public encipherment key of said computer equipment on said list.

38. (currently amended) A system for distributively and dynamically securing a communications network secure, comprising:

a network device interconnected between each computer equipment to be secured and the network, said device comprising:

at least two input/output interfaces for intercepting communications between a computer equipment connected to said device and the network;

an authentication module for obtaining information related to a user of said computer equipment and for defining a security level of said device;

a transmitter for transmitting said information related to the user and said security level of said device to an authentication management server connected to the network;

a storage device; and

a processor; and

~~an~~ wherein said authentication management server connected to the network comprising:

a processor for authenticating the user in accordance with said information related to the user and said security level;

a management device for managing the authentications and the security levels of said devices in said authentication management server; and

a transmitter for distributively transmitting security parameters to ~~each~~ devices on the network; and

wherein said storage device is operable to store said security parameters and said processor of said device is operable to process said security parameters to establish a firewall, thereby distributively and dynamically configuring the security of the network to address new modes of attack.

39. (previously added) The system of claim 38, wherein said security parameters comprise a list of authorized computer client/server applications and information enabling each device to analyze messages related to said client/server applications.

40. (previously added) The system of claim 39, wherein said processor said device comprises:

an analyzer for analyzing the messages related to said client/server applications;

a filter for filtering the messages related to said client/server applications; and

an altering device for altering messages related to said client/server applications.

41. (previously added) The system of claim 38, wherein said security parameters comprise a list of computer equipment which the user is authorized to communicate with.

42. (previously added) The system of claim 41, wherein said processor of said device comprises a controlling device for controlling said device to transmit messages between said computer equipment associated with the user and a computer equipment on said list and to block messages between said computer equipment associated with the user and a computer equipment not on said list.

43. (previously added) The system of claim 38, wherein said authentication module of said device is operable to customize said device in accordance with a private encipherment key; and wherein said server is operable to store all public encipherment keys associated with private encipherment keys which customize the devices.

44. (previously added) The system of claim 43, wherein said security parameters comprise a list of computer equipment and the corresponding public encipherment key which the user is authorized to communicate with, in an enciphered manner.

45. (previously added) The system of claim 44, wherein said device further comprises an encipherment module for enciphering communications between said computer equipment associated with the user and a computer equipment on said list by combining the private encipherment key of said device with the public encipherment key of said computer equipment on said list.

46. (currently amended) A server for distributively and dynamically securing a communications network, comprising:

a processor for processing information and security levels received from a plurality of network devices to authenticate users, each information and security levels being related to a user of a computer equipment connected to a device;

a management device for managing the authentication and security levels of the users; and

a transmitter for transmitting security parameters to said devices, said security parameters establishing a firewall, said server thereby distributively and dynamically configuring the security of the network to address new modes of attack.

47. (previously added) The server of claim 46, wherein said security parameters comprise a list of authorized computer client/server applications and information enabling each device to analyze messages related to said client/server applications.

48. (previously added) The server of claim 46, wherein said security parameters comprise a list of computer equipment which a user is authorized to communicate with.

49. (previously added) The server of claim 46, further comprising a storage device for storing all the public encipherment keys associated with private encipherment keys which customize said devices.

50. (previously added) The server of claim 49, wherein said security parameters comprise a list of computer equipment and the corresponding public encipherment key which the user (U) is authorized to communicate with, in an enciphered manner.

51. (currently amended) A device for securing a communications network secure, said device being interconnected between each computer equipment to be secured and said network, comprising:

at least two input/output interfaces for intercepting communications between a computer equipment connected to said device and the network;

an authentication module for obtaining information related to a user of said computer equipment and for defining the security level of said device,

a transmitter for transmitting information related to the user and said security level of said device to an authentication management server connected to the network;

a storage device for storing security parameters received from said server; and

a processor for processing said security parameters to establish a firewall, thereby distributively and dynamically configuring the security of the network to address new modes of attack.

52. (previously amended) The device of claim 51, wherein said security parameters comprise a list of authorized computer client/server applications and information enabling each device to analyze messages related to said client/server applications.

53. (previously amended) The device of claim 52, wherein said processor further comprising:

an analyzer for analyzing the messages related to said client/server applications;

a filter for filtering the messages related to said client/server applications; and

an altering device for altering messages related to said client/server applications.

54. (previously amended) The device of claim 51, characterized in that the security parameters comprise a list of computer equipment which the user is authorized to communicate with.

55. (previously amended) The device of claim 54, wherein said processor is operable to permit messages to be transmitted between said computer equipment associated with the user and a computer equipment on said list, and operable to block messages between said computer equipment associated with the user and a computer equipment not on said list.

56. (previously amended) The device of claim 51, wherein said authentication module of said device is operable to provide a private encipherment key for customizing said device.

57. (previously amended) The device of claim 56, wherein said security parameters comprise a list of computer equipment and a corresponding public encipherment key which the user is authorized to communicate with, in an enciphered manner.

58. (previously amended) The device of claim 57, further comprising an encipherment module for enciphering communications between said computer equipment associated with the user and a computer equipment on said list by combining the private encipherment key of said device with the public encipherment key of said computer equipment on said list.